

CLAIMS

What is claimed is:

- Sub a1
- 1 1. A method for securely providing information comprising the steps of:
 - 2 (a) receiving information identifying an encrypted personal security device;
 - 3 (b) providing said identified encrypted personal security device;
 - 4 (c) receiving authentication information; and
 - 5 (d) providing decryption information for said personal security device
 - 6 responsive to said authentication information.
 - 1 2. The method of claim 1 wherein steps (a) and (b) comprise:
 - 2 (a) receiving information identifying an encrypted key; and
 - 3 (b) providing said identified encrypted key.
 - 1 3. The method of claim 1 wherein step (a) comprises receiving information
2 identifying an encrypted personal security device, the personal security device
3 comprising information necessary to make a secure network connection between a
4 network client and a network server.
 - 1 4. The method of claim 1 wherein step (a) comprises receiving information
2 identifying an encrypted personal security device, the personal security device
3 comprising information necessary to make a secure virtual private network
4 connection.
 - 1 5. The method of claim 1 further comprising the step of validating said
2 authentication information.
 - 1 6. The method of claim 1 wherein step (b) further comprises the steps of:

2 (b-a) retrieving said personal security device; and

3 (b-b) providing said personal security device.

1 7. The method of claim 6 wherein step (b-a) comprises retrieving said personal
2 security device from an authentication server.

1 8. The method of claim 1 further comprising the step of storing said personal
2 security device on a smartcard.

1 9. The method of claim 1 further comprising the step of storing said decryption
2 information in a volatile memory element.

1 10. The method of claim 1 wherein step (c) comprises receiving time-dependent
2 authentication information.

1 11. A method for accessing secure information comprising the steps of:

2 (a) receiving an encrypted personal security device;

3 (b) receiving decryption information for said personal security device; and

4 (c) decrypting said personal security device.

1 12. The method of claim 11 further comprising the step of using said decrypted
2 personal security device to access said secure information.

1 13. The method of claim 11 wherein receiving step (a) comprises receiving an
2 encrypted personal security device comprising information necessary to make a
3 secure network connection between a network client and a network server.

1 14. The method of claim 11 wherein receiving step (a) comprises receiving an
2 encrypted personal security device comprising information necessary to make a
3 secure virtual private network connection.

1 15. The method of claim 11 further comprising the steps of:
2 (d) transmitting information identifying an encrypted personal security device;
3 and
4 (e) transmitting authentication information.

1 16. The method of claim 15 wherein step (e) comprises transmitting time-dependent
2 authentication information.

1 17. The method of claim 11 further comprising the step of storing said personal
2 security device on a smartcard.

1 18. The method of claim 11 further comprising the step of storing said decryption
2 information in a volatile memory element.

1 19. A method for allowing a network client secure access to information, the method
2 comprising the steps of:
3 (a) requesting, by said network client, a personal security device from a
4 network server, wherein said personal security device comprises encrypted
5 information necessary to make a secure network connection;
6 (b) forwarding, by said network server, said personal security device to said
7 network client; and
8 (c) providing, by said network server, decryption information for said
9 personal security device.

1 20. The method of claim 19 wherein step (b) comprises providing an encrypted
2 personal security device comprising information necessary to make a secure
3 virtual private network connection.

1 21. The method of claim 19 further comprising the steps of:

- 2 (d) forwarding, by said network server said request to an authentication
3 server;
- 4 (e) querying, by said authentication server a user database with said request;
- 5 (f) returning, by said user database a personal security device to said
6 authentication server; and
- 7 (g) forwarding, by said authentication server said personal security device to
8 said network server.

1 22. The method of claim 19 further comprising the steps of:

- 2 (h) obtaining, by said client, authentication information from an
3 authentication token;
- 4 (i) providing, by said client, said authentication information to said
5 authentication server;
- 6 (j) confirming, by said authentication server, the validity of said
7 authentication information;
- 8 (k) retrieving, by said network server, decryption information for said
9 personal security device from a database; and
- 10 (l) providing, by said network server, decryption information for said
11 personal security device to said client.

1 23. The method of claim 22 wherein step (h) comprises obtaining time-dependent
2 authentication information.

1 24. The method of claim 19 further comprising the steps of:

- 2 (m) decrypting, by said client, said personal security device.

1 25. A device for providing secure access to information comprising:

- 2 (a) a first receiver receiving information identifying an encrypted personal
3 security device;
- 4 (b) a first transmitter providing said identified personal security device;
- 5 (c) a second receiver receiving authentication information; and
- 6 (d) a second transmitter providing decryption information for said personal
7 security device responsive to said authentication information.

1 26. The device of claim 25 wherein said receiver receives said encrypted personal
2 security device comprising an encrypted key.

1 27. The device of claim 25 wherein said receiver receives said encrypted personal
2 security device comprising information necessary to make a secure network
3 connection between a network client and a network server.

1 28. The device of claim 25 wherein said receiver receives said encrypted personal
2 security device comprising information necessary to make a secure virtual private
3 network connection.

1 29. The device of claim 25 further comprising an authenticator validating said
2 authentication information.

1 30. The device of claim 25 wherein said first receiver is the same as said second
2 receiver.

1 31. The device of claim 25 wherein said first transmitter is the same as said second
2 transmitter.

1 32. The device of claim 25 wherein said authentication information is time-
2 dependent.

- 1 33. A device for accessing secure information comprising:
2 (a) a first receiver receiving an encrypted personal security device;
3 (b) a second receiver receiving decryption information for said personal
4 security device; and
5 (c) a decryptor decrypting said personal security device.
- 1 34. The device of claim 33 wherein said receiver receives said encrypted personal
2 security device comprising information necessary to make a secure network
3 connection between a network client and a network server.
- 1 35. The device of claim 33 wherein said receiver receives said encrypted personal
2 security device comprising information necessary to make a secure virtual private
3 network connection.
- 1 36. The device of claim 33 further comprising:
2 (d) a first transmitter transmitting information identifying an encrypted
3 personal security device; and
4 (e) a second transmitter transmitting authentication information.
- 1 37. The device of claim 36 wherein said first transmitter is the same as said second
2 transmitter.
- 1 38. The device of claim 36 wherein said authentication information is time-
2 dependent.
- 1 39. The device of claim 33 further comprising a smartcard storing said decryption
2 information.

1 40. The device of claim 33 further comprising a volatile memory element storing said
2 decryption information.

1 41. The device of claim 33 wherein said first receiver is the same as said second
2 receiver.

1 42. A system for providing secure access to information comprising:
2 (a) a network client comprising a volatile memory element; and
3 (b) a network server storing an encrypted personal security device in a server
4 memory element, said personal security device comprising encrypted
5 information.

1 43. The system of claim 42 further comprising a smartcard having a volatile memory
2 element storing said personal security device.

1 44. The system of claim 42 wherein said user database includes said personal security
2 device.

1 45. The system of claim 42 further comprising decrypted information for forming a
2 secure network connection between said client and said server wherein said
3 decrypted information is derived from applying said decryption information to
4 said personal security device.

1 46. The system of claim 42 wherein said decryption information is stored in said
2 volatile storage.

1 47. The system of claim 42 wherein said decrypted information is stored in said
2 volatile storage.

1 48. The system of claim 42 wherein said network is a virtual private network.

1 49. The system of claim 42 wherein said encrypted information comprises
2 information necessary for forming a secure network connection between said
3 client and said server.

1 50. The system of claim 42 further comprising:

2 (c) an authentication token, wherein said token is capable of providing
3 authentication information; and

4 (d) an authentication server, wherein said authentication server comprises a
5 user database, wherein said user database comprises decryption
6 information for said personal security device, and wherein said
7 authentication server is capable of providing said decryption information
8 upon receipt of said authentication information.

1 51. The system of claim 50 wherein said authentication information is time-
2 dependent.